

Verificación del cumplimiento según las estrategias de gobierno, riesgo y cumplimiento

**Breve descripción:**

El logro de objetivos organizacionales es posible en la medida en que se gestionen integralmente los riesgos dentro del cumplimiento de regulaciones nacionales y globales, y también en el marco de las buenas prácticas de gobierno corporativo.

**Diciembre 2023**

Tabla de contenido

[Introducción 1](#_Toc152781984)

[1. Cultura de cumplimiento y gestión de riesgos 4](#_Toc152781985)

[1.1. Gobierno corporativo 6](#_Toc152781986)

[1.2. Gestión de Riesgos 7](#_Toc152781987)

[1.3. Cumplimiento de la regulación 10](#_Toc152781988)

[1.4. Gobierno, Riesgo y Cumplimiento en la era digital 11](#_Toc152781989)

[2. Auditoría de los sistemas de gestiones según la ISO 19011 18](#_Toc152781990)

[3. Sistema de Gestión de Cumplimiento según la ISO 37301 29](#_Toc152781991)

[3.1. Evaluación del desempeño 31](#_Toc152781992)

[Síntesis 37](#_Toc152781993)

[Material complementario 39](#_Toc152781994)

[Glosario 40](#_Toc152781995)

[Referencias bibliográficas 43](#_Toc152781996)

[Créditos 45](#_Toc152781997)

Introducción

En los últimos años, con la globalización y la complejidad de los mercados en la era digital, la incertidumbre ha aumentado significativamente para las organizaciones.

Los problemas éticos en grandes corporaciones, difundidos ampliamente por los medios de comunicación, como los de Enron (2001) y el banco BCCI (1986) de Estados Unidos, y la constructora Odebrecht (2015) en Latino América, han causado perjuicios a los accionistas, a los trabajadores, proveedores, al medio ambiente, y a la sociedad en general. Ante tales escándalos corporativos, las regulaciones nacionales e internacionales han respondido con legislación para evitar se vuelvan a presentar tales delitos. También surgió la necesidad de desarrollar valores, vincularlos a una cultura organizacional de la ética, y así surge el concepto de gobierno corporativo.

Adicionalmente, nuevos elementos se han ido incorporando al panorama empresarial con los cambios en los modelos de negocios, que se aceleraron con motivo de la emergencia sanitaria global (2019); la llamada transformación digital, con el diseño de los productos y servicios centrados en las personas, hizo también que la gestión de gobierno, riesgo y cumplimiento cambiara de foco.

1. Verificación del cumplimiento según las estrategias de gobierno, riesgo y cumplimiento



[**Enlace de reproducción del video**](https://youtu.be/khEG8Ct4JS0)

|  |
| --- |
| Síntesis del video: Verificación del cumplimiento según las estrategias de gobierno, riesgo y cumplimiento |
| Con el cambio de escenario empresarial, los riesgos más retadores para las organizaciones actualmente son ciberseguridad, tecnología y riesgos estratégicos.  Por todo lo anterior, es imprescindible realizar una gestión integral de riesgos dentro del marco de las buenas prácticas de gobierno corporativo.  La gestión de riesgo empresarial es la disciplina que anticipa, detecta, supervisa y mitiga eventos potenciales y oportunidades que afecten el logro de objetivos organizacionales.  El cumplimiento es la disciplina relacionada con el aseguramiento del cumplimiento efectivo de acuerdos, disposiciones internas, reglas y leyes emanados de entes reguladores externos.  Otro concepto es la responsabilidad social, que lleva a considerar que las actividades y decisiones de las organizaciones impactan el bienestar de las comunidades.  El comportamiento ético y con transparencia puede contribuir al desarrollo sostenible de la sociedad.  Según Cascón (2021), con estas disciplinas relacionadas surge el concepto de Gobierno Corporativo, Riesgo y Cumplimiento GRC, para potenciar la efectividad en las empresas.  En este componente formativo, se tratará la razón del gobierno corporativo y la necesidad de gestionar integralmente los riesgos en las organizaciones. También se tratarán orientaciones de las normas ISO 19011:2018 sobre auditoría de sistemas de gestión e ISO 37301:2021 sobre los sistemas de gestión de cumplimiento. |

# Cultura de cumplimiento y gestión de riesgos

Tanto las personas como las organizaciones que deseen ser exitosas necesitan de valores y cumplimiento de normas. Los valores, la cultura y la integridad son los motores para el éxito sostenido de las empresas, bien sean privadas o estatales.

Se dice que una persona demuestra integridad cuando es honesta, actúa correctamente, sin afectar a otros. Los valores de las personas son los determinantes de la cultura de las organizaciones, y la cultura de la organización puede definir los riesgos en el logro de los objetivos.

Las organizaciones y las personas que deseen ser exitosas necesitan una cultura de cumplimiento evidente y genuina. Y los líderes de la organización, directores, gerentes, deberían predicar con el ejemplo, para que la cultura de cumplimiento sea adoptada por todos.

Tradicionalmente, las actividades de gestión de riesgo y el cumplimiento de la regulación se habían ejecutado como funciones independientes, y dado que las normas y los marcos de referencia tanto de gestión de riesgo como de cumplimiento comparten requerimientos comunes, se pueden presentar actividades redundantes y uso ineficiente de recursos.

De la necesidad de manejar las redundancias e ineficiencias surge el programa de GRC, con una visión integral denominada Gobierno, Riesgo y Cumplimento (Governance, Risk and Compliance - GRC), con el cual se deben identificar las correlaciones entre diferentes tipos de riesgos, elementos internos y entes regulatorios, considerando que el entorno es dinámico y tanto los riesgos como los requerimientos de cumplimiento están evolucionando permanentemente.

La siguiente figura ilustra la estrecha relación existente entre Gobierno, Riesgo y Cumplimiento GRC:

**Figura 1.** Gobierno, Riesgo y Cumplimiento GR

Figura 1. Gobierno, Riesgo y Cumplimiento GRC
En la figura se tiene los engranajes de riesgo, gobierno y cumplimiento.

Riesgo.

Gobierno.

Cumplimiento.

## Gobierno corporativo

El gobierno corporativo es el conjunto de normas, principios y procedimientos que regulan la estructura y el funcionamiento de los órganos de gobierno de una empresa. En concreto, establece las relaciones entre la junta directiva, el consejo de administración, los accionistas y el resto de las partes interesadas, y estipula las reglas por las que se rige el proceso de toma de decisiones sobre la compañía para la generación de valor (“Deloitte”, 2022).

El gobierno corporativo responde a las exigencias no solo por parte de inversores, sino también de los consumidores y de la sociedad que requieren saber cómo las organizaciones logran los resultados. Es por esto que cada vez adquiere mayor relevancia que las organizaciones sean gestionadas con transparencia, buenas prácticas y comportamiento responsable, para lograr mayores niveles de confianza y haciéndolas más atractivas, competitivas y sostenibles en el tiempo.

Por el contrario, la falta de buen gobierno corporativo es la causa de reportes de falsos registros contables, contratación sin criterios profesionales, aceptación de sobornos, desvío de dineros a cuentas personales, e innumerables situaciones que se han presentado en organizaciones. El tipo de gobierno corporativo depende del tipo de empresa; por ejemplo, las que cotizan en bolsa son presionadas a tener un gobierno corporativo sólido, requisito de normas de las comisiones de valores de cada jurisdicción.

Sin embargo, las prácticas de gobierno corporativo pueden y deben ser aplicadas a todas las empresas, sin importar el tamaño, porque, como se mencionaba al comienzo, cada vez es más fácil que se divulguen las faltas y sean de conocimiento de clientes y sociedad en general, a través de medios de comunicación y redes sociales, lo que también constituye riesgos reputacionales.

Las normas de gobierno corporativo articulan los componentes siguientes:

1. Toma de decisiones y políticas corporativas.
2. Mecanismos de control sobre el desempeño de la dirección ejecutiva.
3. Cumplimiento del marco normativo.
4. Relaciones entre órganos de gobierno, derechos y deberes de: consejo de administración, junta directiva y accionistas.

En cuanto a empresas del Estado, los principios de buen gobierno, la metodología de gestión del riesgo y el cumplimiento de normas son similares al sector privado, la diferencia principal es que el objetivo no es necesariamente maximizar el valor de los accionistas, sino proveer servicios y productos de acuerdo con los intereses y prioridades definidas por el Estado. Según se describe en DNP (s.f.), la práctica del buen gobierno busca mejores organizaciones, eficiencia de los recursos públicos y procesos de gestión, atracción y promoción de talento humano con excelencia para el servicio público, y mayor transparencia. También se mencionan los principios orientadores del ejercicio del buen gobierno:

* Transparencia y rendición de cuentas.
* Gestión pública efectiva.
* Participación y servicio al ciudadano.
* Vocación por el servicio público.
* Estrategias de lucha contra la corrupción.

## Gestión de Riesgos

Los estándares internacionales definen los riesgos como eventos que impiden el logro de los objetivos de las organizaciones. Y la gestión de riesgo es el conjunto de actividades que la organización realiza para entender y reducir los efectos de la incertidumbre en el logro de los objetivos. Por lo tanto, el primer paso en una gestión de riesgo es entender los objetivos de la organización en particular.

En el proceso de gestión de riesgos se identifican, analizan, mitigan y controlan los riesgos, hasta dejarlos en un nivel residual que sea aceptable por la organización.

La gestión de riesgo tradicionalmente se asocia al análisis cuantitativo, y exige conocimientos de probabilidades, finanzas, estadística y matemáticas. Pero también, por tener elementos de comportamiento humano, la gestión de riesgo requiere del componente psicológico, de habilidades de imaginación y persuasión para comunicar a las partes interesadas.

En la actividad de identificación de los riesgos, estos se pueden agrupar en categorías, que según la función se pueden clasificar de la siguiente manera:

* **Riesgo estratégico**

Se presenta por efecto de la decisión tomada o no respecto al rumbo que sigue la organización. Ejemplos: Son fuentes de riesgo estratégico:

* Implementación de tecnologías emergentes.
* Fusiones y adquisiciones.
* Riesgo reputacional.
* Robo de propiedad intelectual.
* Espionaje industrial.
* **Riesgo financiero**

Relacionado con la pérdida de dinero en una inversión o iniciativa de negocio. Ejemplos:

* Riesgo de liquidez.
* Riesgo de crédito.
* Fraude financiero.
* Lavado de dinero.
* **Riesgo legal y reglamentario**

Resulta de violación de leyes, regulaciones, códigos de conducta o práctica establecidos en una industria u organización.

* **Riesgo operacional**

Fallas de procesos, personas, sistemas y equipos. Ejemplos:

* Configuraciones erróneas.
* Afectación de infraestructura crítica.
* Gestión de proveedores.
* **Riesgo tecnológico**

La tecnología ha potenciado la productividad y también ha expuesto a las organizaciones a nuevos riesgos relacionados con la información. Ejemplos:

* Falla accidental o intencional de componentes tecnológicos.
* Fraude.
* Piratería informática.
* Datos sensibles.
* **Ciberseguridad**

Va más allá del aprovechamiento de una falla o vulnerabilidad de componentes, puede afectar personas, organizaciones y países dadas las características de propagación y evolución, así como la incertidumbre que se puede presentar. Ejemplos:

* Secuestro de datos.
* “Fearware” (manipulación social).
* Fraudes con criptomonedas.
* Ataques usando inteligencia artificial.
* Compromiso de datos en la nube híbrida.

## Cumplimiento de la regulación

El “compliance*”* hace relación a los esfuerzos de las organizaciones por mitigar el riesgo legal. El cumplimiento puede tener una parte de obligaciones de cumplimiento **mandatorias** y otra parte de obligaciones de cumplimiento **voluntarias**.

Las obligaciones de cumplimiento mandatorias se refieren a las leyes que deben cumplir las empresas, pueden ser ambientales, laborales, leyes de lavado de activos, etc. Y las obligaciones de cumplimiento voluntarias están relacionadas con cumplimiento de obligaciones adquiridas por acuerdos con empleados, por ejemplo, obligaciones contractuales, requisitos de norma ISO, directrices, y también relacionadas con mitigar penas por delitos como el cohecho o la colusión, contienen elementos de autorregulación y se refuerzan con códigos internos de conducta (Cascón, 2021).

Cada organización debe cumplir regulaciones según el sector al que pertenece, e históricamente, los servicios financieros han sido de los más exigidos por las regulaciones en todos los países, junto con los de salud, alimentos, minería y transporte.

El riesgo legal se basa en reglas y, por tanto, es manejable con una estrategia de cumplimiento sólida y la implementación de un Sistema de Gestión de Cumplimiento (SGC); las pérdidas financieras por multas y los daños de reputación son evitables. Debido a la aprobación de leyes de responsabilidad penal para las personas jurídicas, en los últimos años, puede ser un mitigante del riesgo legal para las organizaciones tener implementado un SGC.

En términos generales, son elementos clave del programa de cumplimiento:

* El rol del oficial de cumplimiento.
* El mapa de riesgos.
* El plan de comunicación.
* Los códigos internos de conducta.

## Gobierno, Riesgo y Cumplimiento en la era digital

Hoy por hoy, las compañías se transformaron y se adaptaron a las nuevas condiciones, desarrollando nuevos productos y servicios basados en datos y explotando tecnologías emergentes con aplicaciones de blockchain, Big data*,* IoT, Inteligencia Artificial.

Debido al nuevo contexto, la gestión de riesgos debe incluir riesgos emergentes con estas características (SENA, 2020):

* Alta incertidumbre y falta de conocimiento sobre impacto e interacciones.
* Incremento de complejidad, interacciones emergentes y dependencias sistemáticas.
* Cambios en el contexto: político, económico, social, tecnológico y legal.

Se requiere entender el riesgo en el contexto digital, con las características de incertidumbre y complejidad, y aprender de los eventos para el desarrollo de la capacidad de resiliencia. La resiliencia de una organización se desarrolla con la combinación de factores estratégicos y operativos.

“La resiliencia organizacional es la capacidad de una organización para absorber y adaptarse en un entorno cambiante para permitirle cumplir sus objetivos y sobrevivir y prosperar. Las organizaciones más resilientes pueden anticipar y responder a amenazas y oportunidades, que surgen de cambios repentinos o graduales en su contexto interno y externo. Mejorar la resiliencia puede ser un objetivo estratégico de la organización y es el resultado de una buena práctica empresarial y una gestión eficaz del riesgo” (ISO, 2017).

Para generar la confianza digital, las organizaciones, entonces, ahora deben además de contar con el proceso de gestión de seguridad para garantizar la continuidad del negocio, también desarrollar capacidades de resiliencia para lograr mantener la operación del negocio a pesar de haber sido impactados por eventos de ciberseguridad.

**Marcos de referencia y estándares internacionales para el GRC**

El uso de marcos de referencia y estándares permite impulsar programas de Gobierno, Riesgo y Cumplimiento apropiados para cada organización. A continuación, se presentan algunos de los principales relacionados con este programa que se pueden adoptar de manera integral en las organizaciones:

* **COBIT**

Control Objectives for Information and Related Technologies (ISACA, 2019), es un marco de referencia para el gobierno y la gestión de la información y la tecnología empresarial, dirigido a toda la empresa.

Integra varios estándares para procesos específicos, como COSO, para controles internos; ITIL, para alinearse con las necesidades de la empresa; BiSL, enfocada en la demanda de información; el estándar ISO 27000, de seguridad para TI; el entrenamiento en mejoras de procesos, CMMI; TOGAF, para la arquitectura empresarial; y PMBOK, para manejo de proyectos.

* **Modelo de capacidad GRC – OCEG**

Este modelo de capacidad de GRC es el primer y único estándar de código abierto que integra las diversas subdisciplinas de gobierno, riesgo, auditoría, cumplimiento, ética/cultura y TI en un enfoque unificado basado en principios (OCEG, 2022).

Este estándar se puede usar para abordar una variedad de situaciones y áreas temáticas, desde anticorrupción hasta continuidad comercial y administración de terceros. El modelo es una excelente herramienta para enmarcar conversaciones sobre las capacidades de GRC con la junta directiva, los altos ejecutivos y los gerentes.

**Figura 2.** Modelo de capacidad GRC

Figura 2. Modelo de capacidad GRC
En la figura se tiene en el centro interactuar, alrededor en circulo organizar, evaluar, pro actuar, detectar, responder y medir. En el circulo externo el contexto con diseño y organización, gestión de incertidumbre, operación y continuidad, aprendizaje y monitoreo.

**Análisis de la anatomía del modelo de capacidad GRC**

Aprendizaje y monitoreo.

Diseño y organización.

Gestión de incertidumbre.

Operación y continuidad.

**Contexto**

Organizar

Medir.

Interactuar.

Evaluar.  
Responder.

Pro-actuar.

Detectar.

* **Modelo COSO**

Para gestión de riesgos. Sus siglas responden a Committee of Sponsoring Organizations of the Treadway (COSO, 2017), que es una organización de carácter voluntario constituida por representantes de cinco organizaciones del sector privado en Estados Unidos. Nace en 1985 con la misión de crear y proporcionar conocimiento frente a la gestión del riesgo empresarial (ERM), el control interno y la lucha contra el fraude.

**Figura 3.** Modelo COSO

Figura 3. Modelo COSO
En la figura se tiene un cubo, en la base  se tiene ambiente de control, sobre esta capa evaluación de riesgo, luego actividades de control, posteriormente información y comunicación, por último monitoreo.
En la parte superior del cubo se tienen operaciones, informe financiero y cumplimiento, y horizontalmente se tiene Actividad 1 y 2, unidad A y B.


Monitoreo – Operaciones - Informe financiero. – Cumplimiento.

Información y comunicación – actividad 1.

Actividades de control – actividad 2.

Evaluación de riesgos – Unidad A.

Ambiente del control – Unidad B.

* **Modelo de las tres líneas**

Promueve un gobierno sólido y la gestión de riesgos (IIA, 2020). El IIA Instituto de Auditores Internos, en el año 2020, actualizó el modelo de gestión de riesgo y control, “Modelo de las tres líneas de defensa”, por un modelo de interconexión de los roles: Órgano de Gobierno, Gerencia y Auditoría Interna, para asegurar las condiciones de cumplimiento de la organización.

**Figura 4.** Modelo de las tres líneas

Figura 4. Modelo de las tres líneas
En la figura se tiene en la primera línea de defensa: controles de gerencia, medidas de control interno. En la segunda línea de defensa se tiene: controles financieros, seguridad, gestión de riesgos, calidad, inspección y cumplimiento.
en la tercera línea de defensa se tiene la auditoría interna.
Sobre las tres líneas se tiene la alta dirección, luego organismo de Gobierno, consejo, comité de auditoría.
Paralelamente se realiza auditoría externa y organismos de control.

Organismo de gobierno / Consejo /Comité de autoría.

Alta dirección.

**Primera línea de defensa.**

* Controles de gerencia.
* Medidas de control interno.

**Segunda línea de defensa.**

* Controles financieros.
* Seguridad.
* Gestión de riesgos.
* Calidad.
* Inspección.
* Cumplimiento.

**Tercera línea de defensa.**

* Auditoría interna

Auditoría externa.

Organismos de control.

* **Norma ISO 31000:2018**

Contiene los principios y guías para la gestión de riesgo, y define el riesgo, no de la manera tradicional, enfocado en las posibles pérdidas, sino como el efecto de la incertidumbre en los objetivos de la empresa (ISO, 2018). La ISO 31000:2018, aunque no es certificable, permite a las organizaciones de todos los sectores, sin importar que sean públicas o privadas, incorporar estándares y procesos de alto nivel para evaluar y mitigar cualquier tipo de riesgo en todas sus operaciones.

* **ISO 37301:2021**

“Compliance Management System” se crea como respuesta al creciente interés de las empresas por alinear sus sistemas de gestión de cumplimiento de acuerdo con normas internacionales (ISO, 2021). Esta reemplazó a la ISO 19600:2014 “Compliance Management Systems” – Guidelines. El documento especifica los requisitos y proporciona directrices para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión del "compliance" eficaz dentro de una organización. El documento es aplicable a toda clase de organizaciones, independientemente del tipo, tamaño y naturaleza de la actividad, así como a organizaciones del sector público, privado o sin fines de lucro.

Como se vio, son varias las organizaciones de profesionales que han trabajado en los últimos años en el desarrollo y madurez de normas y marcos de referencia. Estas organizaciones, además, ofrecen permanente formación a los asociados y profesionales interesados en adquirir las habilidades y competencias, también ofrecen exámenes de certificación en dichos marcos y normas, con el fin de que los profesionales demuestren su idoneidad para desempeñarse como consultores de los temas de riesgo y cumplimiento.

# Auditoría de los sistemas de gestiones según la ISO 19011

Las auditorías son un proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas de manera objetiva, con el fin de determinar el grado en que se cumplen los criterios de auditoría.

En esta sección, se hace referencia a la norma ISO 19011:2018 (ISO, 2018), que contiene las orientaciones sobre la auditoría de los sistemas de gestión, incluyendo los principios de la auditoría, la gestión de un programa de auditoría y la realización de auditorías de sistemas de gestión, y es aplicable a todas las organizaciones que necesitan planificar y realizar auditorías internas o externas de sistemas de gestión, o gestionar un programa de auditoría.

**Tipos de auditoria**

Con base en la relación con el auditor y el auditado, existen tres tipos de auditoria:

* **Auditorías internas**

Realizadas por personal de la organización, para valorar el Sistema de Gestión implementado. Tienen como enfoque revisar los procesos para detectar oportunidades de mejora en procura de la eficacia de los sistemas de gestión.

* **Auditoría Externa de Procesos**

Su objetivo es evaluar la relación entre el cliente y el proveedor, se revisa que los proveedores cumplan con los requisitos preestablecidos entre ambas partes en el contrato.

* **Auditoría de Conformidad**

Realizadas con el fin de lograr la certificación o acreditación en un sistema de gestión, mantener la certificación o recertificación. También puede tratarse de una auditoria legal o reglamentaria realizada por una agencia gubernamental.

La norma ISO 19011:2018 hace referencia a las auditorías de primera y segunda parte. En algunos casos, se auditan varios sistemas de gestión de distintas disciplinas, por ejemplo: Sistema de Gestión de Calidad- SGC, de Seguridad de la Información- SI, de Gestión Ambiental- SGA, de Seguridad y Salud en el Trabajo- SSST, etc. En esos casos, se le denomina auditoría **combinada.** También se puede presentar la situación de auditar Sistemas Integrados en un único Sistema de Gestión; los principios y procesos de auditoría son los mismos que para una auditoría combinada, a veces llamada auditoría integrada.

**Principios de la auditoría**

Los **principios** de la auditoria son declaraciones de filosofía, reglas o códigos de conducta, en este caso, relacionados con las auditorías:

1. **Integridad**

Fundamento de la profesionalidad.

Se refiere a que las personas que gestionan un programa de auditoría y realizan auditoría desempeñan su labor de forma ética, con honestidad y responsabilidad; solo si son competentes, llevan a cabo las actividades de auditoría; siendo imparciales, es decir, sin sesgo en todas sus acciones y siendo sensibles a cualquier influencia que se pueda ejercer sobre su juicio mientras realiza la auditoría.

1. **Presentación imparcial**

Obligación de informar con veracidad y exactitud.

La comunicación entre auditores y auditado debería ser veraz, exacta, objetiva, oportuna, clara y completa. Se debería informar de los obstáculos significativos encontrados durante la auditoría. Los hallazgos, las conclusiones e informes de la auditoría deberían reflejar con veracidad y exactitud las actividades de auditoría.

1. **Debido cuidado profesional**

Aplicación de diligencia y juicio al auditar.

El cliente de la auditoría y demás partes interesadas depositan confianza en el equipo auditor, y este debe proceder con debido cuidado profesional, demostrando la capacidad de hacer juicios razonados en todas las situaciones de la auditoría.

1. **Confidencialidad**

Seguridad de la información.

Durante la auditoría, el equipo auditor podrá tener acceso a información para realizar las tareas; dicha información no debe usarse inapropiadamente para beneficio personal del auditor o del cliente de la auditoría, y sin perjudicar los intereses legítimos del auditado. La confidencialidad incluye el tratamiento apropiado de la información sensible o confidencial.

1. **Independencia**

Base para la imparcialidad de la auditoría y la objetividad de sus conclusiones.

Los auditores deberían actuar de una manera libre de sesgo y conflicto de intereses. Aun en las auditorías internas, se debe fomentar la objetividad en el proceso de auditoría, y los auditores deberían ser independientes de la función que se audita, para asegurar que los hallazgos y conclusiones están basados solo en la evidencia de la auditoría.

1. **Enfoque basado en la evidencia**

Método racional para alcanzar conclusiones de la auditoría fiables y reproducibles en un proceso de auditoría sistemático.

Auditoría basada en evidencia, porque la evidencia debería basarse en muestras de la información disponible, ya que una auditoría se lleva a cabo durante un periodo de tiempo delimitado y con recursos finitos. Debería aplicarse un uso apropiado del muestreo, para que exista confianza en las conclusiones de la auditoría.

1. **Enfoque basado en riesgos**

Considera los riesgos y oportunidades.

El enfoque basado en riesgos se debe tener en cuenta durante la planificación, la realización y la presentación de los informes de auditoría, con el fin de asegurar que las auditorías se centran en asuntos importantes para la organización y para lograr los objetivos del programa de auditoría.

Los 7 principios de auditoría ayudan a hacer del proceso una herramienta eficaz y fiable en apoyo de las políticas y controles de gestión. Es un requisito para el equipo de auditores adherirse a estos principios para proporcionar conclusiones pertinentes y suficientes de la auditoría realizada.

**Programa de la auditoría**

El programa de auditorías hace referencia a un conjunto de auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico. El programa depende del contexto del auditado, de los objetivos organizacionales, de las necesidades y expectativas de las partes interesadas, de los requisitos de seguridad y confidencialidad de la información.

La información que debe incluir el programa de auditoría se muestra a continuación.

1. Objetivos para el programa de auditoría.
2. Riesgos y oportunidades asociadas con el programa de auditoría y las acciones para abordarlos.
3. Alcance de cada auditoría dentro del programa de auditoría.
4. Calendario (número, duración, frecuencia) de las auditorías.
5. Tipos de auditoría, tales como internas o externas.
6. Criterios de auditoría.
7. Métodos de auditoría a emplear.
8. Criterios para seleccionar a los miembros del equipo auditor.
9. Información documentada pertinente.

**Método establecido en la auditoría**

Elmétodo de auditoríaseleccionado depende de los objetivos de la auditoría, el alcance y los criterios definidos, así como de la duración y la ubicación. También la manera, el lugar y el momento en que se accede a la información de auditoría pueden determinar los métodos de auditoría y, según las circunstancias de la auditoría, pueden mezclar métodos o necesitar cambiarlos durante el proceso.

Según la auditoría se realice en las instalaciones del auditado, in situ, o a distancia, con o sin interacción entre personal auditado y equipo auditor, los métodos de auditoría pueden ser diferentes:

* **En instalaciones con interacción**
* Entrevistas.
* Completar listas de verificación y cuestionarios con la participación del auditado.
* Revisar los documentos con la participación del auditado.
* Muestrear.
* **En instalaciones sin interacción humana**
* Revisar los documentos.
* Observar el trabajo desempeñado.
* Realizar visitas al sitio.
* Completar listas de verificación.
* **A distancia con interacción**
* Entrevistas a través de medios de comunicación interactivos.
* Observar el trabajo realizado con una guía a distancia.
* Completar listas de verificación y cuestionarios a través de medios de comunicación interactivos.
* Revisar los documentos con la participación del auditado a través de medios de comunicación interactivos.
* **A distancia sin interacción humana**
* Revisar los documentos
* Observar el trabajo desempeñado a través de medios de vigilancia, considerando los requisitos sociales y legales.
* Analizar los datos.

Las actividades de auditoría sin interacción humana con las personas que representan al auditado implican la interacción con los equipos, las instalaciones y la documentación, por ejemplo, revisión de registros, análisis de datos y muestrear productos.

La viabilidad de las actividades de auditoría a distancia puede depender del nivel de riesgo para el logro de los objetivos de la auditoría, el nivel de confianza que existe entre el auditor y el personal del auditado, y los requisitos reglamentarios. En las auditorías a distancia, se utilizan medios de comunicación interactivos para realizar las entrevistas, observar el trabajo realizado, completar cuestionarios y listas de verificación junto con el auditado.

**Ciclo PHVA**

Planificar-Hacer-Verificar-Actuar, ciclo PHVA, es una estrategia de mejora continua en 4 pasos, también conocida como ciclo *Deming*.

El ciclo PHVA es una estrategia interactiva de resolución de problemas para mejorar procesos e implementar cambios en las organizaciones, ofrece un alto nivel de flexibilidad y mejora iterativa.

En las normas ISO, se destaca el “enfoque a procesos” y se sugiere el uso de esta metodología como una herramienta de mejora continua. Los auditores deben comprender que auditar un sistema de gestión es auditar los procesos de una organización y sus interacciones con una o más normas de sistemas de gestión.

Cuando las actividades se comprenden y se gestionan como procesos interrelacionados que funcionan como un sistema coherente, se logran resultados coherentes y predecibles de manera más eficaz y eficiente.

**Gestión de un programa de auditoría**

En la gestión del Programa de Auditoría (PA), se cumple el ciclo de la mejora continua PHVA. En el capítulo 5 de la norma ISO 19011, en los numerales 5.2 a 5.7, se describen las actividades que deben seguir las personas responsables de gestionar el programa de auditoría (ISO, 2018).

El capítulo 6 de la norma ISO 19011 (ISO, 2018) comprende desde la preparación y realización de una auditoría, como parte de un programa de auditoría, hasta su seguimiento.

A continuación, se ilustra el **Ciclo PHVA**, incluyendo una breve descripción de los numerales correspondientes a la gestión de un programa y la realización de auditorías:

**Relacionada con la gestión:**

* + **Planificar**

**5.2**. Al planificar, se establecen los objetivos del programa de auditoría, deben ser coherentes con la dirección estratégica de la organización y servir de apoyo a los objetivos y política del Sistema de Gestión que se esté auditando.

**5.3.** El equipo responsable de la gestión del programa de auditoría debe identificar y presentar al cliente de la auditoría los riesgos y oportunidades considerados al desarrollar el programa de auditoría y los requisitos de recursos, para que puedan tratarse adecuadamente; las oportunidades pueden ser relacionadas a fechas según disponibilidad de los auditados, minimizar tiempo, número de visitas, entre otros.

**5.4.** Se definen los roles, responsabilidades y competencias de los responsables del programa de auditoría, se establece la extensión del programa de auditoría, determinando los recursos financieros y de tiempo.

* + **Hacer**

**5.5.** En la implementación del programa de auditoría, se coordinan las actividades, se comunica el programa, se definen e implementan controles necesarios para su seguimiento, identificando mejoras.

Se definen objetivos, alcance y criterios de auditorías individuales, determinando métodos de auditoría y seleccionando miembros del equipo auditor.

Se asignan responsabilidades al líder del equipo auditor, se gestionan resultados del programa de auditorías. Los responsables del programa deben asegurar que generan, gestionan y conservan registros de auditoría.

* + **Verificar**

**5.6.** Se debe asegurar la evaluación del cumplimiento de agendas, logro de objetivos del programa, desempeño del equipo auditor, retroalimentación de los clientes de la auditoría, suficiencia de la información documentada en el proceso de auditoría.

* + **Actuar**

**5.7.** Las personas responsables de la gestión del programa de auditoría y el cliente de la auditoría revisan el programa, también identifican oportunidades de mejora y aplican cambios al programa si es necesario. En esta etapa, también se revisa el desarrollo profesional continuo de los auditores.

**Relacionada con la realización**

* + **Planificar**

**6.2.** La responsabilidad de llevar a cabo la auditoría hasta su finalización es del líder del equipo auditor designado. Al iniciar la auditoría, el líder del equipo auditor hace contacto con el auditado para comunicar canales de comunicación, objetivos, alcance, métodos y equipo de auditoría. También solicita acceso a la información pertinente, determina acuerdos de ubicación, seguridad, entre otros.

**6.3.** Como parte de la preparación de actividades de auditoría, se revisa la información documentada para la comprensión de la operación del auditado, para preparar las actividades y los documentos de trabajo de la auditoría.

Con base en la información, se planifica en detalle la auditoría basada en riesgos, se asignan las tareas al equipo auditor, se prepara la información documentada para la auditoría, como listas de verificación, detalle de muestreo e información audiovisual.

* + **Hacer**

**6.4.** Se asignan roles y responsabilidad a guías y observadores de la auditoría. Se realiza reunión de apertura, se confirma el acuerdo de participantes, el equipo auditor y sus roles, se asegura ejecución de las actividades planeadas, la comunicación durante la auditoría, la disponibilidad y acceso de la información de auditoría. Se recopila, revisa y verifica la información documentada mediante muestreo. Se generan hallazgos, determinan conclusiones de auditoría, se prepara y realiza reunión de cierre.

**6.5.** El líder del equipo auditor debe informar las conclusiones y distribuir el informe de auditoría en los tiempos acordados, de acuerdo con el programa de auditoría.

* + **Verificar**

**6.6.** Finalizando la auditoría, se revisan las lecciones aprendidas, se identifican los riesgos y las oportunidades para el programa de auditoría y para el auditado.

* + **Actuar**

**6.7.** Según los objetivos de auditoría, los resultados pueden indicar la necesidad de correcciones o de acciones correctivas u oportunidades para la mejora, se realizan las actividades de seguimiento de la auditoría, y en una auditoría posterior se puede verificar la eficacia de las acciones llevadas a cabo.

# Sistema de Gestión de Cumplimiento según la ISO 37301

Un SGC comprende: las políticas, los objetivos, y los procesos de “compliance”.

En la implementación de un SGC, como se especifica en la norma ISO 37301:2021 (ISO, 2021), se recorrerán de manera interactiva las fases del ciclo PHVA.

Las normas ISO tienen una estructura común y los numerales de la norma cubren todo el ciclo de la mejora continua, como se muestra en la siguiente figura, los numerales de ISO 37301. Requerimientos y guía de uso para el SGC:

**Figura 5.** Numerales norma ISO 37301 SGC

Figura 6. Numerales norma ISO 37301 SGC
En la figura se tiene:
ACTUAR 
10 Mejora.
PLANIFICAR
4 Contexto de la organización
5 Liderazgo
6 Planificación.
HACER
7 Apoyo
8 Operación.
VERIFICAR
9 Evaluación del desempeño.

**Planificar**

4 contexto de la organización.

5 Liderazgo.

6 Planificación.

**Hacer**

7 Apoyo.

8 Operación.

**Verificar**

9 Evaluación del desempeño.

**Actuar**

10 Mejora.

Para cada numeral de la norma que contiene requisitos (cláusulas 4 al 10), existe una serie de actividades para desarrollar con el equipo de cumplimiento y representantes de los procesos que se abordan. También se realizan capacitaciones en todos los niveles, con el fin de desarrollar la cultura de cumplimiento, porque la responsabilidad del logro de los objetivos de cumplimientos es de todos, no solamente del oficial encargado o quien haga la función.

La implementación del SGC permite a la organización:

* La demostración eficaz, comprobable del cumplimiento de las obligaciones. Por ejemplo, leyes, reglamentos, acuerdos, contratos, código, directrices.
* La buena reputación de la organización.

## Evaluación del desempeño

Una vez implementados los procesos, realizadas las capacitaciones, que estén funcionando los mecanismos para la prevención, la detección y respuesta a situaciones de cumplimiento eventual o real, llega el momento de evaluar el desempeño en función del cumplimiento de los requisitos de la norma ISO 37301.

El desempeño corresponde a los resultados medibles, y se puede relacionar con la gestión de actividades, procesos, productos, servicios, sistemas u organizaciones.

En el numeral 9 de la norma 37301:2021, se describe la evaluación del desempeño del SGC, que corresponde a la fase Verificar (V) del ciclo PHVA.

A continuación, se describen los frentes de la evaluación de desempeño del SGC:

* **Realizar el seguimiento, medición, análisis y evaluación del sistema de gestión**

Es necesario obtener valores para saber si se están logrando los objetivos de cumplimiento que estableció la organización en la fase anterior.

Para ello, se identifican las fuentes de retroalimentación del desempeño, se desarrollan indicadores, se elaboran informes, se mantienen registros.

Se puede decir que se hace seguimiento del sistema de gestión cuando se realizan verificaciones, supervisión y observaciones en forma crítica. Se debe definir a qué hacer seguimiento, cuándo y con cuáles métodos. Asimismo, determinar qué medir, cuándo, y con cuál método.

Se identifican las **fuentes** de información, clientes, proveedores, autoridades, empleados, leyes, auditorías internas, revisiones por la dirección, etc. Y las herramientas para obtener la información pueden ser encuestas de percepción, canales de denuncia, quejas, entre otras.

También se deben desarrollar **indicadores** de gestión apropiados para determinar si se están logrando los objetivos y para evaluar el desempeño en términos de cumplimiento. Los indicadores deben ser claros y comprensibles para todas las personas.

Cada organización puede organizar los indicadores según su conveniencia, su realidad, su contexto, e incluso, su nivel de conocimiento, lo importante es que tales indicadores soporten la toma de decisiones para mejorar el desempeño del SGC. Son ejemplo de indicadores: número de incidentes de protección de datos, tiempo para la investigación de denuncias, número de no conformidades de cumplimiento abiertas, entre otros.

El **informe** de cumplimiento que elabora periódicamente el oficial encargado o el equipo que tenga la función, sobre la base de criterios definidos, lo entrega al órgano de gobierno y a la alta dirección. La gestión eficaz del informe respectivo podría evitar que un problema de no cumplimiento se propague por la organización.

Algunas características del informe son:

* Debe detallar la obligación y cumplimiento correspondiente y los no cumplimientos que se produjeron.
* Mencionar los requisitos de las partes interesadas.
* Señalar las acciones correctivas implementadas y su eficacia.
* Mostrar los cambios eventuales en las obligaciones de cumplimiento y en el sistema de comunicaciones a utilizar, además de señalar antecedentes de auditorías y realizar monitoreo de los planes de acción para la mejora.

Los **registros** son parte de la información documentada del sistema de gestión, demuestran seguimientos y mediciones de los procesos. Corresponden a actas de revisión por la dirección, análisis de indicadores de gestión, seguimiento a las acciones correctivas, y los mismos informes de cumplimiento.

* **Auditorías internas**

La auditoría se trata de un proceso planeado, con objetivo establecido y enfocada en procesos. La auditoría debe ser transparente y hacer parte de un plan de auditoría.

En las auditorías, se revisa qué tan confiable es la organización, si respeta los pactos, cumple las promesas organizacionales y las normas.

La ejecución de la auditoría está a cargo del equipo auditor, con base en los conocimientos de los criterios de “compliance”, los requisitos y el contexto del auditado.

Los auditores deben tener habilidades y competencias para realizar la auditoría y una conducta profesional acorde con su rol, que garantice un ambiente de confianza.

La auditoría no debe ser solo un ejercicio burocrático sin sentido, debe ser bien ejecutada, a la vez que entrega valor a la organización con la presentación de acciones apropiadas contenidas en el informe de auditoría. Este informe, es una entrada importante para las decisiones de la alta dirección, que potencialmente influyen en la gestión estratégica de la organización. El documento escrito debe demostrar el logro de los objetivos de auditoría, debe demostrar la eficacia del SGC, y debe identificar las no conformidades en el sistema de gestión y también las oportunidades de mejora.

Después de la auditoría interna, sigue la implementación de acciones correctivas para cerrar las no conformidades detectadas, lo cual es una oportunidad de aprendizaje para la organización (Thaller y Bravo, 2021).

La siguiente figura ilustra tanto el proceso como los elementos de entrada y salida de una auditoría:

**Figura 6.** Proceso de auditoría

Figura 7. Proceso de auditoría
En la figura se representa:
En la parte izquierda las entradas:
Auditores competentes
Conocimiento de la norma
Procedimientos documentados, responsabilidades definidas
Criterios de auditoría, métodos
Luego en el centro de la figura se tiene:
Planeación, ejecución, preparación del informe, comunicación de informe, seguimiento y recomendaciones.
En la parte derecha de la figura se tienen las salidas:
Registros de auditoría
Informes de no conformidad y acciones correctivas
Datos para análisis de oportunidades de mejora
En la parte de abajo una flecha con herramientas utilizadas.

**Entradas**

* Auditores competentes.
* Conocimiento de la norma.
* Procedimientos documentados, responsabilidades definidas.
* Criterios de auditorías, métodos.

**Planeación**

**Ejecución**

**Preparación del informe**

**Comunicación de informe**

**Seguimiento de recomendaciones**

**Herramientas utilizadas**

* Lista de verificación de cumplimiento de los requisitos de la norma.
* Preguntas cruzadas a personas de diferentes procesos y personas clientes de cada proceso.

**Salidas**

* Registros de auditoría.
* Informes de no conformidad y acciones correctivas.
* Datos para análisis de oportunidades de mejora.
* **Revisiones por la Dirección**

La revisión por la dirección es un proceso liderado por la alta dirección y el órgano de gobierno, donde se toman las decisiones relacionadas con las oportunidades de mejora y aplicación de cambios, con el objetivo de mejorar el SGC.

En la revisión por la dirección, se reconoce:

* Si las personas entienden la política de cumplimiento.
* Si se tomaron en cuenta los resultados de auditoría.
* Si las no conformidades fueron resueltas y cuáles acciones correctivas fueron implementadas.
* Se revisa la eficacia de los controles.
* Se toman en cuenta todos los registros frente a la violación de obligaciones de cumplimiento.
* Se evalúa si fueron suficientes los recursos asignados al SGC.

Síntesis

El logro de los objetivos organizacionales es posible en la medida en que se desarrolle una cultura de cumplimiento y se gestionen integralmente los riesgos, dentro del marco de las buenas prácticas de gobierno corporativo. La implementación del sistema de gestión basado en la norma ISO 37301 se puede apoyar de buenas prácticas de los marcos de referencia relacionados con la gestión de riesgo, de gobierno TI y gobierno corporativo. En la evaluación del SGC, se realizan actividades de seguimiento, medición, análisis y evaluación, así como auditorías internas y la revisión por la dirección.

A continuación, se presenta una síntesis de las temáticas vistas en el componente formativo, a través del siguiente mapa conceptual.

Síntesis
En la figura de la síntesis se tiene inicialmente gobierno, riesgo, cumplimiento, que incluye visión integral de cultura de cumplimiento en organizaciones, personas y valores e integridad. También hace parte el gobierno corporativo que corresponde a normas para la toma de decisiones, relaciones entre partes interesadas, gestión de riesgo, y cumplimiento de regulación. De la misma forma se implementa las Normas ISO 31000 y Normas ISO 37301, en la fase de verificación. Para terminar el GRC se apoya en marcos COBIT, COSO, Modelo IIA, GRC Capability model.

Material complementario

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia | Tipo de material | Enlace del recurso |
| 1. Cultura de cumplimiento y gestión de riesgos. | SENA. (2020). Aplicabilidad de Caso Práctico en Gobierno, Riesgo y Cumplimiento - GRC - SENA (Video). YouTube. | Video | <https://www.youtube.com/watch?v=yguzJDDvjDA> |
| 2. Auditoría de los sistemas de gestión según la ISO 19011 | ISO Expertos. (2016). Los 11 secretos para realizar una auditoría que agregue valor (Video). YouTube. | Video | <https://www.youtube.com/watch?v=fN5nC7uGNFc> |

Glosario

**Arquitectura:** conjunto de elementos, sus interrelaciones y factores externos que gobiernan su diseño, su comportamiento y su evolución.

**BiSL- “Business Information Services Library”:** marco utilizado para la gestión de la información regida por la Fundación ASL BiSL (anteriormente, ASL Foundation).

**CIO – “Chief Information Officer”:** director de tecnologías de la información y las comunicaciones, es el ejecutivo que se encarga de que la organización logre el mejor rendimiento posible a través del uso de tecnologías de la información (TI).

**CISO –“Chief Information Security Officer”**: rol desempeñado a nivel ejecutivo, corresponde al director de seguridad de la información.

**Cibernética:** permite conceptualizar la comunicación como una ciencia de relaciones y mediaciones socio técnicas entre seres humanos y objetos de diferente naturaleza.

**Cohecho:** este delito consiste en el soborno a un funcionario público, nacional o extranjero.

**Colusión:** es el delito de ponerse de acuerdo para defraudar al Estado.

**Eficacia:** grado en el que se realizan las actividades planificadas y se logran los resultados planificados.

**ISO- Organización Internacional de Normalización:** federación mundial de organismos nacionales de normalización, que, a través de comités técnicos de ISO, elabora Normas Internacionales.

**Marcos de referencia:** conjunto de métodos, herramientas y lenguaje común.

**Mandatorio/a:** del inglés “mandatory”, y este del lat. tardío “mandatorius”, relativo a un mandato o encargo. Sinónimos: obligatorio, forzoso.

**Resiliencia:** capacidad de absorber y adaptarse en un entorno cambiante. (ISO, 2017)

**Riesgos cibernéticos:** los ciberriesgos son riesgos que tienen al menos tres características claves: son sistémicos (tienen efecto en cascada), emergentes (surgen como fruto del nivel de acoplamiento e interacción de diversos componentes) y disruptivos (generan efectos inesperados sobre la dinámica del sistema), los cuales están presentes en el entorno ciberfísico, lo que se traduce en una convergencia entre lo físico, lo lógico y lo biológico, como fundamento de la dinámica de la Cuarta Revolución Industrial. (Cano, 2019)

**Gobierno, Riesgo y Cumplimento –GRC:** OCEG (2022) define a GRC como "la colección integrada de capacidades que permiten a una organización alcanzar objetivos de manera confiable, abordar la incertidumbre y actuar con integridad".

**Transformación Digital:** es la adaptación continua de los negocios a las exigencias del entorno cambiante. Es un enfoque centrado en el cliente que utiliza tecnologías digitales para aprovechar los datos e impulsar flujos de trabajo inteligentes. Entre las tecnologías utilizadas actualmente y en el futuro cercano, tenemos la Inteligencia Artificial, la automatización, IoT, nube híbrida, Blockchain y Microservicios.

El objetivo de la transformación digital es construir una base técnica y operativa para evolucionar y responder de la mejor manera posible a las expectativas impredecibles y cambiantes de los clientes, las condiciones del mercado y los eventos locales o globales.

**Tráfico de influencias:** es el intercambio de un bien por la promesa de interceder en el ámbito judicial.

Referencias bibliográficas

Cano, J. (2019). Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo. *Revista SISTEMAS. Asociación Colombiana de Ingenieros de Sistemas*, (151), p. 63-73. <https://doi.org/10.29236/sistemas.n151a5>

Cascón, J. (2021). *GRC Gobierno Corporativo, Riesgo y Cumplimiento*. <https://www.researchgate.net/profile/Javier-Ismodes-2/publication/348280507_GRC_JIC_v70/links/5ff6225e45851553a02626da/GRC-JIC-v70.pdf>

Deloitte. (s. f.). *¿Qué es el gobierno corporativo? Transparencia y confianza*. <https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/que-es-el-gobierno-corporativo.html>

Departamento Nacional de Planeación [DNP]. (s. f.). Rutas especializadas para la formulación de los Planes de Desarrollo Territoriales. *Buen Gobierno.* <https://www.funcionpublica.gov.co/documents/418537/28834001/Rutas+Especializadas+Buen+Gobierno.pdf/3eb8f83c-dec8-3d4e-461b-84f68a836591>

Fundación Latinoamericana de Auditores Internos [FLAI]. (2020). *El Modelo de las Tres Líneas del IIA 2020*. <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-spanish.pdf>

ISACA. (s. f.). COBIT. An ISACA Framework. <https://www.isaca.org/resources/cobit>

ISO Expertos. (2018). *Los 11 secretos para realizar una auditoría que agregue valor* (Video). YouTube. <https://www.youtube.com/watch?v=fN5nC7uGNFc>

OCEG. (s. f.). What Is GRC (Governance, Risk, and Compliance)? <https://www.oceg.org/about/what-is-grc/>

Organización Internacional de Normalización [ISO]. (2017). *Security and resilience — Organizational resilience —* Principles and attributes (ISO 22316). <https://www.iso.org/obp/ui#iso:std:iso:22316:ed-1:v1:en>

Organización Internacional de Normalización [ISO]. (2018a). *Directrices para la auditoría de los sistemas de gestión* (ISO 19011). <https://www.iso.org/obp/ui#iso:std:iso:19011:ed-3:v1:es>

Organización Internacional de Normalización [ISO]. (2018b). *Gestión del riesgo – Directrices* (ISO 31000)*.* <https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es>

Organización Internacional de Normalización [ISO]. (2021). Compliance management systems *—* Requirements with guidance for use(ISO 37301)*.* <https://www.iso.org/obp/ui/#iso:std:iso:37301:ed-1:v1:es>

SENA. (2020). *Aplicabilidad de Caso Práctico en Gobierno, Riesgo y Cumplimiento - GRC - SENA* (Video). YouTube. <https://www.youtube.com/watch?v=yguzJDDvjDA>

Thaller, E. y Bravo, J. (2021). Beyond Compliance*: Aplicación de la Norma ISO 37301 en cualquier organización interesada en el* compliance*.* Paton Professional. <https://books.google.com.co/books?id=-dxCEAAAQBAJ&pg=PT60&hl=es&source=gbs_selected_pages&cad=2#v=onepage&q&f=false>

Créditos

| Nombre | Cargo | Regional y Centro de Formación |
| --- | --- | --- |
| Claudia Patricia Aristizábal | Responsable del Equipo | Dirección General |
| Norma Constanza Morales Cruz | Responsable de Línea de Producción | Regional Tolima - Centro de Comercio y Servicios |
| Dolly Stella Carrillo Vega | Experta Temática | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios |
| Gustavo Santis Mancipe | Diseñador Instruccional | Regional Distrito Capital –  Centro de Gestión Industrial |
| Silvia Milena Sequeda Cárdenas | Asesora Pedagógica y Metodológica | Regional Distrito Capital –  Centro de Diseño y Metrología |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo Desarrollo Curricular | Regional Santander -  Centro Industrial del Diseño y la Manufactura |
| Darío González | Corrector de Estilo | Regional Distrito Capital –  Centro de Diseño y Metrología |
| Juan Guillermo Zuluaga Saavedra | Expero Temático | Regional Tolima -  Centro de Comercio y Servicios |
| Humberto Arias Díaz | Diseñador Instruccional | Regional Tolima -  Centro de Comercio y Servicios |
| María Inés Machado López | Asesora Metodológica | Regional Tolima -  Centro de Comercio y Servicios |
| José Yobani Penagos Mora | Diseñador Web | Regional Tolima – Centro de Comercio y Servicios |
| Oscar Daniel Espitia Marín | Desarrollador Fullstack | Regional Tolima – Centro de Comercio y Servicios |
| Gilberto Junior Rodríguez Rodríguez | Storyboard e Ilustración | Regional Tolima – Centro de Comercio y Servicios |
| María Alejandra Vera Briceño | Productor y Animador Audiovisual | Regional Tolima – Centro de Comercio y Servicios |
| Nelson Iván Vera Briceño | Productor y Animador Audiovisual | Regional Tolima – Centro de Comercio y Servicios |
| Oleg Litvin | Productor y Animador Audiovisual | Regional Tolima – Centro de Comercio y Servicios |
| Oscar Daniel Espitia Marín | Actividad Didáctica | Regional Tolima – Centro de Comercio y Servicios |
| Jorge Bustos Gómez | Validación y Vinculación en Plataforma LMS | Regional Tolima – Centro de Comercio y Servicios |
| Gilberto Naranjo Farfán | Validación de Contenidos Accesibles | Regional Tolima – Centro de Comercio y Servicios |